


[Advanced Search](#) [Preferences](#) [Language Tools](#) [Search Tips](#)

remote administrate telecommunication

Google Search

[Web](#) - [Images](#) - [Groups](#) - [Directory](#) - [News](#)
Searched the web for **remote administrate telecommunication**.Results **1 - 10** of about **601**. Search took **0.19** seconds

Internet / Connectivity / Remote Administration

... REAL TIME and allows you to **administrate** the **remote** ... standard RADIUS server and a **remote** manage client ... and can be used for **telecommunication** accounting platform ...
freedownloadswindows.com/windows/Remote-Administration/6796/ - 22k - [Cached](#) - [Similar pages](#)

Sponsored Links

Telecom Jobs & Resumes

Search Thousands of Jobs, Post your Resume on TelecomCareers.Net!
www.telecomcareers.net
 Interest: [\[Link\]](#)

The Medical Web White Paper

... to the hospital, one for the **remote** office, and ... Figure 2 Sharing **Telecommunication** Lines. ... cost of an Information System department to **administrate** the number of ...
www.med-web.com/mwproj/whitepaper/WhitePaper.html - 55k - [Cached](#) - [Similar pages](#)

Telecommunications

Browse exporter catalogs online.
 Forbes Magazine "Best of the Web".
www.alibaba.com
 Interest: [\[Link\]](#)

Program upravljanja, nadzora i održavanja

... are modem' connections (host/**remote**-pcAnywhere), zg ... a leading role in **telecommunication** network data ... control, observe, maintenance and **administrate** assisting. ...
www.tel.hr/hpt-split/puno/puno10e.htm - 7k - [Cached](#) - [Similar pages](#)

Original Remote Controls

Repair Service Available
 Hard to find Original Remotes
www.replacementremotes.co
 Interest: [\[Link\]](#)

Data Personnel - Job Vacancies

... switches, network management, **remote** access, VPNs, LAN ... by a regional **telecommunication** service provider. ... Duties : - Supervision and **administrate** switch Network. ...
www.hkstar.com/~dpdp/tc.html - 84k - [Cached](#) - [Similar pages](#)

[See your message here...](#)

PDF Design a middleware architecture to provide telecommunication ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 12 Chapter 1 Introduction 1.1 **Telecommunication** services trend Improvements in **telecommunication** network infrastructures, evolution of digital technologies and ...
beethoven.site.uottawa.ca/dsrg/PublicDocuments/REPORTS-THESES/Thesis-DupreLaTour.pdf - [Similar pages](#)

OTE - Community Support Frameworks

... other non urban areas and even **remote** areas for the ... settlements) or even supply of **telecommunication** services to ... that is, the need to **administrate** the spectrum ...
www.ote.gr/oteweb/english/network/gkps.htm - 19k - [Cached](#) - [Similar pages](#)

Product Overview

... reliability in data and **telecommunication** applications because it ... See "**Remote Switch** Modules," for the technical ... extension chassis to **administrate** systems with ...
www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/opguide/intro.htm - 27k - [Cached](#) - [Similar pages](#)

work-at-home-jobs-and-employment.com

... Data and **Telecommunication** workstation adds, moves and changes ... **Administrate** and maintain NT workstation systems for ... 103 users with local and **remote** desktop PCs ...
www.work-at-home-jobs-and-employment.com/resumes_admin_001.php - 25k - [Cached](#) - [Similar pages](#)

Impact Voice Mail Server - Black Ice Software Inc.

... maintenance cost through advanced **remote** administration using a ... had a distinct **telecommunication** advantage over ... market that lets you **administrate** voice servers ...
www.blackice.com/vserversandard.htm - 48k - Jun 26, 2003 - [Cached](#) - [Similar pages](#)

Innovaphone Home Page

... **remote** configuration. ... The gateway can **administrate** voice calls and route them ... can be integrated into a company's existing **telecommunication** infrastructure, the ...

Goooooooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

remote administrate telecommunication

Google Search

[Search within results](#)

Dissatisfied with your search results? [Help us improve.](#)

[Google Home](#) - [Advertise with Us](#) - [Business Solutions](#) - [Services & Tools](#) - [Jobs, Press, & Help](#)

©2003 Google

This is Google's cache of <http://www.cert.org/security-improvement/practices/p073.html>.

Google's cache is the snapshot that we took of the page as we crawled the web.

The page may have changed since that time. Click here for the [current page](#) without highlighting.

To link to or bookmark this page, use the following url: http://www.google.com/search?q=cache:rHjxUf_biZMJ:www.cert.org/security-improvement/practices/p073.html+remote+administration&hl=en&ie=UTF-8

Google is not affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: **remote administration**



[Home](#) [Site Index](#)

[vulnerabilities,
incidents & fixes](#)

[Search](#) [Contact](#)

[security practices
& evaluations](#)

[FAQ](#)

[survivability
research & analysis](#)

[training &
education](#)

Configure computers for secure remote administration.

A [practice](#) from the CERT® [Security Improvement Modules](#)

Administration of a workstation or network server includes updating user account information, examining the logs, installing new or updated software, and maintaining an appropriate configuration. These tasks can be performed locally from the workstation or server console, but they can also be performed remotely from a separate host via a network connection.

Although local **administration** is more secure (and we recommend it whenever feasible), **remote administration** is more common, particularly when servicing a large number of workstations or network servers (such as print servers and file servers). When performing **remote administration**, you need to consider the security of the **administration** host, the network, and the workstation or server being administered.

Why this is important

Remote administration of computers is increasingly common because of the significant cost benefits—many tasks can be automated, and the administrator does not have to physically visit each computer. However, **remote administration** tools must be configured to operate securely.

Although the normal operational state of your computer may be secure, during the performance of administrative tasks, your computer may be in a transient vulnerable state. This is especially true for **remote administration** of public servers that have been placed outside your firewall, because this requires that you open a network connection through the firewall. Such a connection may be vulnerable to some forms of attack, and it may open the door to anyone on the Internet being able to "administer" your server. The result could be the loss of confidentiality or integrity of information resources on the server, an intruder gaining access to resources on your internal network, or an intruder being able to use your server or workstation as an intermediate host for attacks on other internal or external hosts.

How to do it

Ensure that the computer accepts administration commands only from an authenticated administrator.

Configure the computer to use a strong method to authenticate the identity of the user who is initiating the administrative processes. In particular, avoid authentication methods that require the transmission of a password in clear text, unless it is a one-time password.

Ensure that the computer allows administration from only an authenticated host.

Authenticate the host in a manner that does not depend on network-resolved information such as IP addresses or DNS names, because intruders can falsify such information within packets sent to computers being administered. We recommend the use of public key authentication using a tool such as secure shell (SSH).

See also the module Securing Public Web Servers [Kossakowski 00], specifically the practice Configure the Web server to use authentication and encryption technologies, where required. This practice briefly covers SSL (Secure Socket Layer), S/HTTP (Secure HTTP), and SET (Secure Electronic Transaction) for use with public Web servers.

Ensure that all administration tasks operate at the minimum necessary privilege level.

Administration tasks sometimes require increased privilege levels. Take care to raise privilege levels only as needed.

Consider separation of duties among administrators which will allow you to assign privilege levels as needed. This eliminates the risk of one administrator becoming a single point of vulnerability.

Ensure that confidential information cannot be intercepted, read, or changed by intruders.

This includes **administration** commands and system configuration information.

Methods such as encryption help to ensure that network packets travelling between the administrator's host machine and the computer being administered would not, if intercepted, provide sensitive information or permit system commands to be altered. Such actions could allow subsequent access to either the computer or your organization's internal network. We recommend the use of SSH or an equivalent encryption tool.

Use a movable storage medium to transfer information from the authoritative copy to public servers outside your firewall.

For some network servers, particularly those providing public services such as WWW, it is common to develop the information content of those services on a different host machine. The authoritative version of that content is maintained (and backed up) on that other machine, and then transferred to the public server at appropriate intervals. The transfer can be performed by using a movable storage medium. This could include a writable CD-ROM, diskette, hard disk cartridge, or tape. Since this procedure does not require a network connection through your firewall, it is more secure.

If a network connection is required, use an encrypted, authenticated VPN connection.

During the transfer, you may need to stop or disable your server. Some servers can be configured to continue operating and to send a "Service temporarily unavailable" message in response to all requests.

Do not use a transfer method that mounts a file system from a host inside the firewall on a public server host (such as a Web server) using NFS. There are inherent problems in the NFS protocol that could make that internal host vulnerable to attack.

Correspondingly, do not use an NFS-based transfer method in the opposite direction (from public server to internal host). This could result in making your public server vulnerable to attack.

Use a secure method for inspecting all log files.

If you choose to inspect the computer log files

- on a host other than the computer that generated the logs, use a secure method for transferring these logs. Movable storage media and file encryption are two suitable methods.
- by remotely accessing the computer from another host, use appropriate authentication and encryption technologies as described above

- by remotely accessing a central log host that contains all log files, use appropriate authentication and encryption technologies as described above

After making any changes in a computer's configuration or in its information content, create new cryptographic checksums or other integrity-checking baseline information for your server.

See the module [Detecting Signs of Intrusion](#) [Allen 00] to find additional information on the role of checking the integrity of baseline information in support of intrusion detection.

Policy considerations

Your organization's security policy for networked systems should

- require the use of secure procedures for **administration** of network servers and workstations
- specify the circumstances under which third parties (vendors, service providers) are permitted to remotely administer your systems and how such **administration** is to be conducted. ¹

Implementation details

[Installing and securing Solaris 2.6 servers](#)

[Installing, configuring, and operating the secure shell \(SSH\) on systems running Solaris 2.x](#)

Footnotes

¹ Refer to the module [Security of Information Technology Service Contracts](#) [Allen 98].

[\[back to top\]](#) [\[full list of modules, practices, and implementations\]](#)

Copyright 2000 Carnegie Mellon University.

[See the conditions for use, disclaimers, and copyright information.](#)

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office.

This page was last updated on May 2, 2001.